

AMENDED IN ASSEMBLY JUNE 14, 2016

AMENDED IN SENATE MARCH 29, 2016

SENATE BILL

No. 1121

Introduced by Senator Leno

February 17, 2016

An act to amend Sections ~~1546.1~~ 1546, 1564.1, and 1546.2 of the Penal Code, relating to privacy.

LEGISLATIVE COUNSEL'S DIGEST

SB 1121, as amended, Leno. Privacy: electronic communications: search warrant.

Existing law prohibits a government entity from compelling the production of or access to electronic communication information or electronic device information, as defined, without a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant to specified conditions, except for emergency situations, as defined. Existing law also specifies the conditions under which a government entity may access electronic device information by means of physical interaction or electronic communication with the device, such as pursuant to a search warrant, wiretap order, or consent of the owner of the device.

This bill would additionally authorize a government entity, without a warrant or other order, to access electronic device information by means of physical interaction or electronic communication with the device ~~in response to a contact made by a member of the public using a 911 emergency communications system~~ for the purpose of accessing information concerning the location of the electronic device ~~that initiated that contact~~. *in order to respond to an emergency 911 call. The bill would also provide that the definition of "electronic device" for*

purposes of the bill does not include a magnetic strip on a driver's license or identification card, as prescribed.

Existing law authorizes a service provider to voluntarily disclose electronic communication information or subscriber information. Existing law requires a government entity to destroy that information within 90 days unless one or more specified circumstances apply, including, among others, the *government* entity has or obtains the specific consent of the sender or recipient of the electronic communications about which information was disclosed.

This bill would also authorize a government entity to retain the information beyond 90 days if the service provider or subscriber is, *or discloses to*, a federal, state, or local prison, jail, or juvenile detention facility, and all parties to the electronic communication were informed, prior to the communication, that the service provider may disclose the information to the *government* entity.

Vote: majority. Appropriation: no. Fiscal committee: yes.
State-mandated local program: no.

The people of the State of California do enact as follows:

- 1 *SECTION 1. Section 1546 of the Penal Code is amended to*
- 2 *read:*
- 3 1546. For purposes of this chapter, the following definitions
- 4 apply:
- 5 (a) An “adverse result” means any of the following:
- 6 (1) Danger to the life or physical safety of an individual.
- 7 (2) Flight from prosecution.
- 8 (3) Destruction of or tampering with evidence.
- 9 (4) Intimidation of potential witnesses.
- 10 (5) Serious jeopardy to an investigation or undue delay of a
- 11 trial.
- 12 (b) “Authorized possessor” means the possessor of an electronic
- 13 device when that person is the owner of the device or has been
- 14 authorized to possess the device by the owner of the device.
- 15 (c) “Electronic communication” means the transfer of signs,
- 16 signals, writings, images, sounds, data, or intelligence of any nature
- 17 in whole or in part by a wire, radio, electromagnetic, photoelectric,
- 18 or photo-optical system.
- 19 (d) “Electronic communication information” means any
- 20 information about an electronic communication or the use of an

1 electronic communication service, including, but not limited to,
2 the contents, sender, recipients, format, or location of the sender
3 or recipients at any point during the communication, the time or
4 date the communication was created, sent, or received, or any
5 information pertaining to any individual or device participating in
6 the communication, including, but not limited to, an IP address.
7 Electronic communication information does not include subscriber
8 information as defined in this chapter.

9 (e) “Electronic communication service” means a service that
10 provides to its subscribers or users the ability to send or receive
11 electronic communications, including any service that acts as an
12 intermediary in the transmission of electronic communications, or
13 stores electronic communication information.

14 (f) “Electronic device” means a device that stores, generates,
15 or transmits information in electronic form. *An electronic device*
16 *does not include the magnetic strip on a driver’s license or an*
17 *identification card issued by this state or a driver’s license or*
18 *equivalent identification card issued by another state.*

19 (g) “Electronic device information” means any information
20 stored on or generated through the operation of an electronic
21 device, including the current and prior locations of the device.

22 (h) “Electronic information” means electronic communication
23 information or electronic device information.

24 (i) “Government entity” means a department or agency of the
25 state or a political subdivision thereof, or an individual acting for
26 or on behalf of the state or a political subdivision thereof.

27 (j) “Service provider” means a person or entity offering an
28 electronic communication service.

29 (k) “Specific consent” means consent provided directly to the
30 government entity seeking information, including, but not limited
31 to, when the government entity is the addressee or intended
32 recipient or a member of the intended audience of an electronic
33 communication. Specific consent does not require that the
34 originator of the communication have actual knowledge that an
35 addressee, intended recipient, or member of the specific audience
36 is a government entity.

37 (l) “Subscriber information” means the name, street address,
38 telephone number, email address, or similar contact information
39 provided by the subscriber to the provider to establish or maintain
40 an account or communication channel, a subscriber or account

1 number or identifier, the length of service, and the types of services
2 used by a user of or subscriber to a service provider.

3 **SECTION 1.**

4 *SEC. 2.* Section 1546.1 of the Penal Code is amended to read:

5 1546.1. (a) Except as provided in this section, a government
6 entity shall not do any of the following:

7 (1) Compel the production of or access to electronic
8 communication information from a service provider.

9 (2) Compel the production of or access to electronic device
10 information from any person or entity other than the authorized
11 possessor of the device.

12 (3) Access electronic device information by means of physical
13 interaction or electronic communication with the electronic device.
14 This section does not prohibit the intended recipient of an electronic
15 communication from voluntarily disclosing electronic
16 communication information concerning that communication to a
17 government entity.

18 (b) A government entity may compel the production of or access
19 to electronic communication information from a service provider,
20 or compel the production of or access to electronic device
21 information from any person or entity other than the authorized
22 possessor of the device only under the following circumstances:

23 (1) Pursuant to a warrant issued pursuant to Chapter 3
24 (commencing with Section 1523) and subject to subdivision (d).

25 (2) Pursuant to a wiretap order issued pursuant to Chapter 1.4
26 (commencing with Section 629.50) of Title 15 of Part 1.

27 (3) Pursuant to an order for electronic reader records issued
28 pursuant to Section 1798.90 of the Civil Code.

29 (4) Pursuant to a subpoena issued pursuant to existing state law,
30 provided that the information is not sought for the purpose of
31 investigating or prosecuting a criminal offense, and compelling
32 the production of or access to the information via the subpoena is
33 not otherwise prohibited by state or federal law. Nothing in this
34 paragraph shall be construed to expand any authority under state
35 law to compel the production of or access to electronic information.

36 (c) A government entity may access electronic device
37 information by means of physical interaction or electronic
38 communication with the device only as follows:

39 (1) Pursuant to a warrant issued pursuant to Chapter 3
40 (commencing with Section 1523) and subject to subdivision (d).

1 (2) Pursuant to a wiretap order issued pursuant to Chapter 1.4
2 (commencing with Section 629.50) of Title 15 of Part 1.

3 (3) With the specific consent of the authorized possessor of the
4 device.

5 (4) With the specific consent of the owner of the device, only
6 when the device has been reported as lost or stolen.

7 (5) If the government entity, in good faith, believes that an
8 emergency involving danger of death or serious physical injury to
9 any person requires access to the electronic device information.

10 (6) If the government entity, in good faith, believes the device
11 to be lost, stolen, or abandoned, provided that the *government*
12 entity shall only access electronic device information in order to
13 attempt to identify, verify, or contact the owner or authorized
14 possessor of the device.

15 (7) Except where prohibited by state or federal law, if the device
16 is seized from an inmate's possession or found in an area of a
17 correctional facility ~~under the jurisdiction of the Department of~~
18 ~~Corrections and Rehabilitation or a secure area of a local detention~~
19 ~~facility where inmates have access and~~ *access*, the device is not in
20 the possession of an ~~individual~~ *individual*, and the device is not
21 known or believed to be the possession of an authorized visitor.
22 Nothing in this paragraph shall be construed to supersede or
23 override Section 4576.

24 ~~(8) In response to a contact made by a member of the public~~
25 ~~using a 911 emergency communications system, but only to access~~
26 ~~information concerning the location of the electronic device that~~
27 ~~initiated that contact.~~

28 *(8) If the government entity accesses information concerning*
29 *the location or the telephone number of the electronic device in*
30 *order to respond to an emergency 911 call.*

31 (d) Any warrant for electronic information shall comply with
32 the following:

33 (1) The warrant shall describe with particularity the information
34 to be seized by ~~specifying the time periods covered and, specifying,~~
35 as appropriate and reasonable, *the time periods covered*, the target
36 individuals or accounts, the applications or services covered, and
37 the types of information ~~sought~~. *sought, provided, however, that*
38 *in the case of a warrant described in paragraph (1) of subdivision*
39 *(c), the court may determine that it is not appropriate to specify*
40 *time periods because of the specific circumstances of the*

1 *investigation, including, but not limited to, the nature of the device*
2 *to be searched.*

3 (2) The warrant shall require that any information obtained
4 through the execution of the warrant that is unrelated to the
5 objective of the warrant shall be sealed and *shall not be* subject to
6 further review, use, or disclosure ~~without a court order.~~ *except*
7 *pursuant to a court order or to comply with discovery as required*
8 *by Sections 1054.1 and 1054.7.* A court shall issue such an order
9 upon a finding that there is probable cause to believe that the
10 information is relevant to an active investigation, or review, use,
11 or disclosure is required by state or federal law.

12 (3) The warrant shall comply with all other provisions of
13 California and federal law, including any provisions prohibiting,
14 limiting, or imposing additional requirements on the use of search
15 warrants. If directed to a service provider, the warrant shall be
16 accompanied by an order requiring the service provider to verify
17 the authenticity of electronic information that it produces by
18 providing an affidavit that complies with the requirements set forth
19 in Section 1561 of the Evidence Code. Admission of that
20 information into evidence shall be subject to Section 1562 of the
21 Evidence Code.

22 (e) When issuing any warrant or order for electronic information,
23 or upon the petition from the target or recipient of the warrant or
24 order, a court may, at its discretion, do either or both of the
25 following:

26 (1) Appoint a special master, as described in subdivision (d) of
27 Section 1524, charged with ensuring that only information
28 necessary to achieve the objective of the warrant or order is
29 produced or accessed.

30 (2) Require that any information obtained through the execution
31 of the warrant or order that is unrelated to the objective of the
32 warrant be destroyed as soon as feasible after the termination of
33 the current investigation and any related investigations or
34 proceedings.

35 (f) A service provider may voluntarily disclose electronic
36 communication information or subscriber information when that
37 disclosure is not otherwise prohibited by state or federal law.

38 (g) If a government entity receives electronic communication
39 information voluntarily provided pursuant to subdivision (f), it

1 shall destroy that information within 90 days unless one or more
2 of the following circumstances apply:

3 (1) The *government* entity has or obtains the specific consent
4 of the sender or recipient of the electronic communications about
5 which information was disclosed.

6 (2) The *government* entity obtains a court order authorizing the
7 retention of the information. A court shall issue a retention order
8 upon a finding that the conditions justifying the initial voluntary
9 disclosure persist, in which case the court shall authorize the
10 retention of the information only for so long as those conditions
11 persist, or there is probable cause to believe that the information
12 constitutes evidence that a crime has been committed.

13 (3) The *government* entity reasonably believes that the
14 information relates to child pornography and the information is
15 retained as part of a multiagency database used in the investigation
16 of child pornography and related crimes.

17 (4) The service provider or subscriber ~~is is, or discloses the~~
18 *information to*, a federal, state, or local prison, jail, or juvenile
19 detention facility, and all ~~parties participants~~ to the electronic
20 communication were informed, prior to the communication, that
21 the service provider may disclose the information to the
22 *government* entity.

23 (h) If a government entity obtains electronic information
24 pursuant to an emergency involving danger of death or serious
25 physical injury to a person, that requires access to the electronic
26 information without delay, the *government* entity shall, within
27 three court days after obtaining the electronic information, file
28 with the appropriate court an application for a warrant or order
29 authorizing obtaining the electronic information or a motion
30 seeking approval of the emergency disclosures that shall set forth
31 the facts giving rise to the emergency, and if applicable, a request
32 supported by a sworn affidavit for an order delaying notification
33 under paragraph (1) of subdivision (b) of Section 1546.2. The court
34 shall promptly rule on the application or motion and shall order
35 the immediate destruction of all information obtained, and
36 immediate notification pursuant to subdivision (a) of Section
37 1546.2 if ~~such~~ *that* notice has not already been given, upon a
38 finding that the facts did not give rise to an emergency or upon
39 rejecting the warrant or order application on any other ground.
40 *This subdivision does not apply if the government entity obtains*

1 *information concerning the location of the electronic device in*
2 *order to respond to an emergency 911 call.*

3 (i) This section does not limit the authority of a government
4 entity to use an administrative, grand jury, trial, or civil discovery
5 subpoena to do any of the following:

6 (1) Require an originator, addressee, or intended recipient of
7 an electronic communication to disclose any electronic
8 communication information associated with that communication.

9 (2) Require an entity that provides electronic communications
10 services to its officers, directors, employees, or agents for the
11 purpose of carrying out their duties, to disclose electronic
12 communication information associated with an electronic
13 communication to or from an officer, director, employee, or agent
14 of the entity.

15 (3) Require a service provider to provide subscriber information.

16 (j) *Nothing in this chapter shall be construed to alter the*
17 *authority of a government entity that owns an electronic device to*
18 *compel an employee who is authorized to possess the device to*
19 *return the device to the government entity's possession.*

20 ~~SEC. 2.~~

21 *SEC. 3.* Section 1546.2 of the Penal Code is amended to read:

22 1546.2. (a) Except as otherwise provided in this section, any
23 government entity that executes a warrant, or obtains electronic
24 information in an emergency pursuant to Section 1546.1, shall
25 serve upon, or deliver to by registered or first-class mail, electronic
26 mail, or other means reasonably calculated to be effective, the
27 identified targets of the warrant or emergency request, a notice
28 that informs the recipient that information about the recipient has
29 been compelled or requested, and states with reasonable specificity
30 the nature of the government investigation under which the
31 information is sought. The notice shall include a copy of the
32 warrant or a written statement setting forth facts giving rise to the
33 emergency. The notice shall be provided contemporaneously with
34 the execution of a warrant, or, in the case of an emergency, within
35 three court days after obtaining the electronic information.

36 (b) (1) When a warrant is sought or electronic information is
37 obtained in an emergency under Section 1546.1, the government
38 entity may submit a request supported by a sworn affidavit for an
39 order delaying notification and prohibiting any party providing
40 information from notifying any other party that information has

1 been sought. The court shall issue the order if the court determines
2 that there is reason to believe that notification may have an adverse
3 result, but only for the period of time that the court finds there is
4 reason to believe that the notification may have that adverse result,
5 and not to exceed 90 days.

6 (2) The court may grant extensions of the delay of up to 90 days
7 each on the same grounds as provided in paragraph (1).

8 (3) Upon expiration of the period of delay of the notification,
9 the government entity shall serve upon, or deliver to by registered
10 or first-class mail, electronic mail, or other means reasonably
11 calculated to be effective as specified by the court issuing the order
12 authorizing delayed notification, the identified targets of the
13 warrant, a document that includes the information described in
14 subdivision (a), a copy of all electronic information obtained or a
15 summary of that information, including, at a minimum, the number
16 and types of records disclosed, the date and time when the earliest
17 and latest records were created, and a statement of the grounds for
18 the court's determination to grant a delay in notifying the
19 individual.

20 (c) If there is no identified target of a warrant or emergency
21 request at the time of its issuance, the government entity shall
22 submit to the Department of Justice within three days of the
23 execution of the warrant or issuance of the request all of the
24 information required in subdivision (a). If an order delaying notice
25 is obtained pursuant to subdivision (b), the government entity shall
26 submit to the department upon the expiration of the period of delay
27 of the notification all of the information required in paragraph (3)
28 of subdivision (b). The department shall publish all those reports
29 on its Internet Web site within 90 days of receipt. The department
30 may redact names or other personal identifying information from
31 the reports.

32 (d) Except as otherwise provided in this section, nothing in this
33 chapter shall prohibit or limit a service provider or any other party
34 from disclosing information about any request or demand for
35 electronic information.